CWNP

CWAP-404 Exam

Certified Wireless Analysis Professional

Thank you for Downloading CWAP-404 exam PDF Demo

You can buy Latest CWAP-404 Full Version Download

https://www.certkillers.net/Exam/CWAP-404

Version: 4.0

Question: 1

Which one of the following should be the first step when troubleshooting a WLAN issue?

A. Identify probable causes
B. Identify capture locations
C. Perform an initial WLAN scan and see if any obvious issues stand out
D. Define the problem

Answer: D

Explanation:

The first step in any troubleshooting process is to define the problem. This involves gathering information from various sources, such as users, network administrators, network documentation, and network monitoring tools. Defining the problem helps to narrow down the scope of the issue and identify the symptoms, causes, and effects of the problem12 Reference:
CWAP-403 Study Guide, Chapter 1: Troubleshooting Methodology, page 7
CWAP-403 Objectives, Section 1.1: Define the problem

Question: 2

Which one of the following is an advantage of using display filters that is not an advantage of capture-time filters?

A. They allow for focused analysis on just the packets of interest
B. Once created they are reusable for later captures
C. They only hide the packets from view and the filtered packets can be enabled for view later
D. Multiple of them can be applied simultaneously

Answer: C

Explanation:

Display filters are applied after the capture is completed and they only hide the packets from view. The filtered packets are still present in the capture file and can be enabled for view later by changing or removing the display filter. This is an advantage over capture-time filters, which discard the packets that

do not match the filter criteria and cannot be recovered later34 Reference:
CWAP-403 Study Guide, Chapter 2: Protocol Analysis, page 37
CWAP-403 Objectives, Section 2.3: Apply display filters

Question: 3

Using a portable analyzer you perform a packet capture next to a client STA and you can see that the STA is associated to a BSS. You observe the STA sending packets to the AP and the AP sending packets to the ST
A. Less than 2% of all packets are retransmissions. You move to capture packets by the AP and, while the retry rate is still less than 2%, you now only see unidirectional traffic from the AP to the client. How do you explain this behavior?
A. The portable analyzer is too close to the AP causing CCI, blinding the AP to the clients packets
B. The STA is transmitting data using more spatial streams than the potable analyzer can support
C. There is a transmit power mismatch between the client and the AP and while the client can hear the APs traffic, the AP cannot hear the client
D. The portable analyzer has a lower receive sensitivity than the AP and while it can't capture the packets from the client STA, the AP can receive them OK

Answer: D

Explanation:

Receive sensitivity is the minimum signal level that a receiver can detect and decode. Different devices may have different receive sensitivity levels depending on their hardware specifications and antenna configurations. In this scenario, the portable analyzer has a lower receive sensitivity than the AP, meaning that it requires a stronger signal to capture the packets from the client STA. The AP, on the other hand, has a higher receive sensitivity and can receive the packets from the client STA even if they have a weaker signal. This explains why the portable analyzer can only see unidirectional traffic from the AP to the client when capturing near the AP5 Reference:
CWAP-403 Study Guide, Chapter 4: PHY Layer Analysis, page 121
CWAP-403 Objectives, Section 4.3: Analyze PHY layer metrics

Question: 4

Given a protocol analyzer can decrypt WPA2-PSK data packets providing the PSK and SSID are configured in the analyzer software. When performing packet capture (in a non-FT environment) which frames are required in order for PSK frame decryption to be possible?

A. Authentication
B. 4-Way Handshake
C. Reassociation
D. Probe Response

Answer: B

Explanation:

The 4-way handshake is the process that establishes the pairwise transient key (PTK) between the client and the AP in WPA2-PSK. The PTK is derived from the PSK, the SSID, and some random numbers exchanged in the handshake frames. The PTK is used to encrypt and decrypt the data frames between the client and the AP. Therefore, in order to decrypt WPA2-PSK data packets, a protocol analyzer needs to capture the 4-way handshake frames and have the PSK and SSID configured in the analyzer software12 Reference:
CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 87
CWAP-404 Objectives, Section 3.5: Analyze security exchanges

Question: 5

When configuring a long-term, forensic packet capture and saving all packets to disk which of the following is not a consideration?

A. Real-time packet decodes
B. Analyzer location
C. Total capture storage space
D. Individual trace file size

Answer: A

Explanation:

Real-time packet decodes are not a consideration when configuring a long-term, forensic packet capture and saving all packets to disk. Real-time packet decodes are useful for live analysis and troubleshooting, but they consume CPU and memory resources that could affect the performance of the capture process. For a long-term, forensic packet capture, it is more important to consider the analyzer location, the total capture storage space, and the individual trace file size. These factors affect the quality and quantity of the captured packets and the ease of post-capture analysis34 Reference:
CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 49
CWAP-404 Objectives, Section 2.1: Configure protocol analyzers

Thank You for trying CWAP-404 PDF Demo

To try our CWAP-404 Full Version Download visit link below

https://www.certkillers.net/Exam/CWAP-404

Start Your CWAP-404 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your CWAP-404 preparation with actual exam questions.